PACIFIC TRIAL ATTORNEYS
A Professional Corporation
Scott J. Ferrell, Bar No. 202091
sferrell@pacifictrialattorneys.com
4100 Newport Place Drive, Ste. 800
Newport Beach, CA 92660
Tel: (949) 706-6464
Fax: (949) 706-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

ARISHA BYARS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SEPHORA USA INC., a Delaware corporation d/b/a WWW.SEPHORA.COM,

Defendant.

Case No. 5:23-cv-883

CLASS ACTION COMPLAINT

INTRODUCTION

Defendant secretly enables and allows a third-party spyware company to wiretap and eavesdrop on the private conversations of everyone who communicates through the chat feature at www.sephora.com (the "Website"). The spyware company then exploits and monetizes that data by sharing it with other third parties, who use the private chat data to bombard the unsuspecting visitor with targeted marketing.

Defendant does this without visitors' informed consent. As a result, Defendant has violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 *et seq*.

JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1332 of the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is at least minimal diversity because at least one Plaintiff and Defendant are citizens of different states. Indeed, based upon the information available to Plaintiff, there are believed to be at least 50,000 class members, each entitled to $5,000 in statutory damages, thus making the amount in controversy at least $250,000,0000 exclusive of interests and costs. *See* Cal. Penal Code § 637.2(a)(1).

2. Pursuant to 28 U.S.C. § 1391, venue is proper because a substantial part of the acts and events giving rise to the claims occurred in this District. Plaintiff and many class members reside in this District.

3. Defendant is subject to personal jurisdiction because it has sufficient minimum contacts with California. Defendant is subject to jurisdiction under California's "long-arm" statute found at California Code of Civil Procedure Section 410.10 because the exercise of jurisdiction over Defendant is not "inconsistent with the Constitution of this state or the United States." Indeed, Plaintiff believes that Defendant

generates a minimum of eight percent of its national website sales to Californians, such that the Website "is the equivalent of having a brick-and-mortar store in California – a 'virtual store.'" *Thurston v. Fairfield Collectibles of Georgia, LLC*, 53 Cal. App. 5th 1231, 1240 (2020) (citing *Stomp, Inc. v. NeatO, LLC*, 61 F. Supp. 2d 1074, 1078 n.7 (C.D. Cal. 1999)). Since this case involves wrongdoing related to the operation of Defendant's Website, which functions as an online store selling goods and products including headphones, earbuds, gaming headsets, and related accessories, California courts can "properly exercise personal jurisdiction" over Defendant in accordance with the Court of Appeal opinion in *Thurston v. Fairfield Collectibles of Georgia, LLC*, 53 Cal. App. 5th 1231, 1237-42 (2020).

PARTIES

4. Plaintiff is a resident and citizen of California who resides in this Judicial District. While physically within California during mid-2022, Plaintiff visited Defendant's Website using a smart phone and conducted a brief conversation with an agent of Defendant through the Website's chat feature. Plaintiff was not advised that the chat was monitored, intercepted, or recorded.

5. Defendant is the U.S. operating subsidiary of a French multinational retailer of personal care and beauty products with nearly 340 brands with its headquarters in California. With hundreds of stores and annual sales in the billions, it is one of America's largest specialty retailers.

6. Defendant owns, operates, and/or controls the above-referenced Website.

FACTUAL ALLEGATIONS

7. CIPA prohibits both wiretapping and eavesdropping of electronic communications without the consent of all parties to the communication. "'[T]he right to control the nature and extent of the firsthand dissemination of [one's] statements'" is viewed by the California Supreme Court "as critical to the purposes of Section 631[.]" *Javier v. Assurance IQ, LLC*, 2023 WL 114225, at *6 (N.D. Cal. Jan. 5, 2023) (Breyer, J.) (quoting *Ribas v. Clark*, 38 Cal. 3d 355, 361 (1985)); *Ribas*, 38 Cal. 3d at 360-61 ("a

substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device"). "[U]nder Section 631, it has always mattered who is holding the tape recorder[.]" *Javier*, 2023 WL 114225, at *6. Compliance with CIPA is easy, and most website operators comply by conspicuously warning visitors if their conversations are being recorded, intercepted, or eavesdropped upon.[1]

8. Unlike most companies, Defendant *ignores* CIPA. Instead, Defendant enables and allows a third party that has no corporate affiliation with Defendant to eavesdrop on all such conversations. Why? Because, as one industry expert notes, "*Live chat transcripts are the gold mines of customer service. At your fingertips, you have valuable customer insight to make informed business decisions. . . .**When people are chatting, you have direct access to their exact pain points.***"). *See* https://www.ravience.co/post/improve-marketing-roi-live-chat-transcripts (last visited May 16, 2023) (emphasis added).

9. Defendant's actions are not incidental to facilitating e-commerce, nor are they undertaken in the ordinary course of business. To the contrary, as noted above, Defendant's actions violate industry norms and the legitimate expectations of consumers.

10. To enable the eavesdropping, Defendant has allowed a third party to covertly embed code into Defendant's chat feature. On information and belief, the third party is a company named "LiveChat" and is hereafter referred to as the "Third Party Spyware Company." See https://www.livechat.com/customers/customer-stories/sephora/ (quoting Sephora executive Milena Wojewoda explaining that Sephora

[1] https://www.leechtishman.com/insights/blog/the-california-invasion-of-privacy-act-californias-wiretap-act/ ("A business must take certain steps, as part of its privacy program, to ensure that ***any time the business is gathering***, either automatically, or ***with a chat feature***, ***personal data of a consumer/website visitor***, ***that it obtains valid consent consistent with the holdings and determinations of the courts interpreting CIPA*** and other applicable Data Privacy laws.") (last visited May 11, 2023) (emphasis added).

chose LiveChat because *"We liked the intuitive and easy-to-use interface, as well as the fact that we could give our customers the chance to rate our consultants. More importantly, we can monitor the quality of customer service thanks to advanced analytics.*").

11. The secret code is a type of automatic routing software that automatically acquires and transmits user chat communications to the Third Party Spyware Company without any active input from either Defendant's employees, agents, or human representatives or the Third Party Spyware Company's employees, agents, or human representatives. Third Party Spyware Company acquired website visitors' chat communications by rerouting them to computer servers that it owns, controls, and maintains. The secret code enables and allows the Third Party Spyware Company to secretly intercept in real time, eavesdrop upon, and store transcripts of Defendant's chat communications with unsuspecting website visitors – even when such conversations are private and personal. Defendant neither informs visitors of this conduct nor obtains their consent to these intrusions.

12. One might reasonably wonder why a Third Party Spyware Company would be interested in intercepting and recording the website chat interactions between Defendant and unsuspecting visitors to Defendant's Website. As shown below, it all about money.

13. The Third Party Spyware Company's chat software is "integrated" with Meta, Inc.'s subsidiaries like Facebook and WhatsApp. (Integration allows various software sub-systems to share data to operate as a unified system). According to Bloomberg.com, this is all part of Meta's secret "***plan to profit from private chats.***" As Bloomberg explained, Meta's software integration "*can manage customer messages from multiple services on one central dashboard. That's central to Meta's plan to make money off of its two messaging apps, WhatsApp and Messenger.*" *See* https://www.bloomberg.com/news/articles/2022-02-15/meta-closes-1-billion-kustomer-deal-after-regulatory-review (last downloaded March 2023).

14. So how does it work? ***First***, Meta identifies "user interests" by monitoring a collection of "offsite" user activity such as website visits and interactions (including private chat communications between Defendant and visitors) by "integrating" its software with the Third Party Spyware Company's software. ***Second***, Meta generates revenue by selling advertising space through its subsidiaries' ability to identify those offsite user interests. ***Third and finally***, after the chat transcripts intercepted by the Third Party Spyware Company are provided to Meta through "integration", Meta brands like Facebook and WhatsApp bombard the unsuspecting website visitors with targeted advertising based upon the user's website visits and interactions.

15. Indeed, Defendant recently updated its online privacy policy to admit to the sum and substance of Plaintiff's claims. *See* https://www.sephora.com/beauty/privacy-policy#USPersonalInformation. (*"We maintain a transcript of chats for quality assurance. . . we use personal information for marketing and promotional purposes, such as to show you advertisements for products and/or services tailored to your interests on social media and other websites."*) (last accessed May 16, 2023).

16. Indeed, all of the schemers – Defendant, the Third Party Spyware Company, and Meta – all profit from secretly exploiting the private chat data through targeted social media advertising because "*Targeted advertising allows brands to send different messaging to different consumers based on what the brand knows about the customer. The better a brand can demonstrate that it understands what its customers want and need, the more likely customers respond to advertising and engage with the brand. . . . Social media targeting helps brands leverage consumers' behavior on the web, search engines, and social media sites to present ads that reflect consumer interests.*"[2]

17. The Third Party Spyware Company does more than merely provide a

[2] *See* https://www.adroll.com/blog/what-is-targeted-advertising#:~:text=Targeted%20advertising%20allows%20brands%20to,and%20engage%20with%20the%20brand (last visited May 16, 2023).

storage function for Defendant regarding Website users' chat communications with Defendant. Third Party Spyware Company uses its record of Website users' interaction with Defendant's chat feature for purposes other than storage including data analytics and marketing/advertising to consumers. In addition, Third Party Spyware Company has the capability to use its record of Website users' interaction with Defendant's chat feature for purposes other than storage including data analytics and marketing/advertising to consumers. The Third Party Spyware Company's exploitation, monetization, use of, and interaction with the data it gathers through the chat feature on Defendant's Website in real time makes it a third party under Section 631 as opposed to a party.

18. Given the nature of Defendant's business, Plaintiff (and all visitors) share PII and personal and confidential data with Defendant via the Website chat feature.

19. Within the last year, Plaintiff visited Defendant's Website. Plaintiff used a smart phone (a cellular telephone with integrated computers to enable web browsing). As such, Plaintiff's conversations with Defendant were transmitted from "cellular radio telephones" as defined by CIPA.

20. By definition, Defendant's chat communications from its Website are transmitted to website visitors by either cellular telephony or landline telephony. *See* https://www.britannica.com/technology/Internet ("How does the Internet work?") ("*The Internet works through a series of networks that connect devices around the world through telephone lines.*") (last visited May 16, 2023) (emphasis added).

21. Defendant did not inform Class members that Defendant was secretly allowing, aiding, and abetting the Third Party Spyware Company to intercept and eavesdrop on the conversations during transmission, or that the Third Party Spyware Company provided data from such transcripts to Meta through "integration" with Meta software.

22. Defendant did not obtain Plaintiff's or the Class members' express or implied consent for the preceding intrusions, nor did Plaintiff or Class members know at the time of the conversations of Defendant's conduct.

CLASS ALLEGATIONS

23. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class") defined as follows:

> **All persons within the United States who within the statute of limitations period: (1) communicated with Defendant via the chat feature on Defendant's Website; and (2) whose communications were recorded and/or eavesdropped upon without prior consent.**

24. NUMEROSITY: Plaintiff does not know the number of Class members but believes the number to be in the thousands, if not more. The exact identities of Class members may be ascertained by the records maintained by Defendant.

25. COMMONALITY: Common questions of fact and law exist as to all Class members, and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class member, include but are not limited to the following:

a. Whether Defendant aided and abetted a third party in eavesdropping on such communications;

b. Whether Plaintiff and Class members are entitled to statutory penalties; and

c. Whether Class members are entitled to injunctive relief.

26. TYPICALITY: As a person who visited Defendant's Website and whose electronic communication was recorded, intercepted and eavesdropped upon, Plaintiff is asserting claims that are typical of the Class.

27. ADEQUACY: Plaintiff will fairly and adequately protect the interests of the members of The Class. Plaintiff has retained attorneys experienced in the class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the class or whose inclusion would otherwise be improper are excluded.

28. SUPERIORITY: A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class members is impracticable and inefficient. Even if every Class member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

FIRST CAUSE OF ACTION

Violations of the California Invasion of Privacy Act

Cal. Penal Code § 631(a)

29. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

30. "Any person who, by means of any machine, instrument, or contrivance, or in any other manner, [i] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [ii] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [iii] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [iv] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine . . . ." *Yoon v. Lululemon*

USA, Inc., 549 F. Supp. 3d 1073, 1080 (C.D. Cal. 2021) (Holcomb, J.) (line breaks and headings of clauses added for ease of reference) (quoting Cal. Penal Code § 631(a)).

31. Section 631 of the California Penal Code applies to internet communications and thus applies to Plaintiff's and the Class's electronic communications with Defendant's Website. "Though written in terms of wiretapping, Section 631(a) applies to Internet communications. It makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.'" *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. 2022); *Yoon*, 549 F. Supp. 3d at 1080 ("Courts agree … that CIPA § 631 applies to communications conducted over the internet.") (citing *Matera v. Google Inc.*, 2016 WL 8200619, at *18 (N.D. Cal. Aug. 12, 2016) (Koh, J.) (holding that second clause of section 631(a) "encompasses email communications, which pass over wires, lines, or cables")); *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013) (Koh, J.) ("the Court finds that section 631 of CIPA applies to emails"); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 826 (N.D. Cal. 2020) (Labson Freeman, J.).

32. The Third Party Spyware Company's software embedded on Defendant's Website to record and eavesdrop upon the Class's communications qualifies as a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct alleged herein. *See In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 937 (N.D. Cal. 2015) (stating that "***it is undeniable that a computer may qualify as a 'machine'***" within the meaning of section 631(a)) (emphasis added), *aff'd in part and rev'd in part on other grounds*, 956 F.3d 589 (9th Cir. 2020).

33. At all relevant times, Defendant intentionally caused the internet communication between Plaintiff and Class Members with Defendant's Website to be recorded. Defendant also aided and abetted, agreed with, employed, or conspired with at least one third party to wiretap and/or eavesdrop upon such conversations during

transmission and in real time by voluntarily embedding the software code for Third Party Spyware Company's software on Defendant's Website.

34. Defendant knows that Third-Party Spyware Company, through software, captures the electronic communications of visitors to Defendant's Website, and pays Third-Party Software Company to conduct these activities.

35. Plaintiff and Class Members did not expressly or impliedly consent to any of Defendant's or Third Party Spyware Company's actions.

36. In a materially identical case, a court recently held that the above-described allegations state viable claims for violations of section 631(a) of CIPA. *See Byars v. The Goodyear Tire & Rubber Co.*, No. 5:22-cv-01358-SSS-KKx, 2023 WL 1788553, at *4 (C.D. Cal. Feb. 3, 2023) (Sykes, J.) ("*Byars contends that Goodyear, using a third-party service, "intercepts in real time" a website visitors' chat conversation. . . . Byars alleges that, using the chat conversation, website visitors share sensitive personal information. . . . . Because Byars has pled sufficient facts to show the contents of the communications and that the communications were intercepted, Byars has sufficiently stated a claim under § 631(a).*") (emphasis added).

37. Defendant's conduct constitutes numerous discrete violations of Cal. Penal Code § 631(a), entitling Plaintiff and/or Class Members to injunctive relief and statutory damages.

SECOND CAUSE OF ACTION

Violations of the California Invasion of Privacy Act

Cal. Penal Code § 632.7

38. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

39. Section 632.7 of California's Penal Code imposes liability upon anyone "who, without the consent of all parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cellular radio telephones, a

cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone."

40. Plaintiff and the class members communicated with Defendant using telephony subject to the mandates and prohibitions of Section 632.7.

41. Defendant's communication from the chat feature on its Website is transmitted via telephony subject to the mandates and prohibitions of Section 632.7.

42. As set forth above, Defendant recorded telephony communication without the consent of all parties to the communication in violation of Section 632.7.

43. As set forth above, Defendant also aided and abetted a third party in the interception, reception, and/or intentional recordation of telephony communication in violation of Section 632.7.

44. In a materially identical case, a court recently held that the above-described allegations state viable claims for violations of section 632.7 of CIPA. *See Byars v. The Goodyear Tire & Rubber Co.*, No. 5:22-cv-01358, 2023 WL 1788553, at *5 (C.D. Cal. Feb. 3, 2023) (Sykes, J.) ("*Byars' alleged communication with Goodyear occurred via Goodyear's chat feature on its website. Byars accessed Goodyear's website using her smartphone. As smartphones are cellular phones with web capabilities, Byars' smartphone falls within the cellular phone category. . . . Because Byars' contends that users of Goodyear's website "share highly sensitive personal data" via Goodyear's chat feature, Byars has sufficiently alleged that website users had a reasonable expectation of privacy and therefore the communications fall within the scope of § 632.7.*") (emphasis added and internal citations omitted).

45. Defendant's conduct constitutes numerous discrete violations of Cal. Penal Code § 632.7, entitling Plaintiff and/or Class members to injunctive relief and statutory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief against Defendant:

1. An order certifying the Class, naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class counsel;
2. An order declaring Defendant's conduct violates CIPA;
3. An order of judgment in favor of Plaintiff and the Class and against Defendant on the causes of action asserted herein;
4. An order enjoining Defendant's conduct as alleged herein and any other injunctive relief that the Court finds proper;
5. Statutory damages pursuant to CIPA;
6. Reasonable attorneys' fees and costs; and
7. All other relief that would be just and proper as a matter of law or equity, as determined by the Court.

Dated: May 16, 2023

PACIFIC TRIAL ATTORNEYS, APC

By: */s/ Scott J. Ferrell*
Scott. J. Ferrell
Attorneys for Plaintiff